Who's watching your network

DNS Security Ready for Prime Time

2000 June

Olafur Gudmundsson <ogud@tislabs.com>
Edward P. Lewis <lewis@tislabs.com>
NAI Labs

Main Problem:
Retrofitting security into complex and fragile infrastructure protocol (DNS) and get it deployed!!

Joint Government and Industry Support for Reference Implementation

- Open, Standards Based DNS Security
- Standards Defined Through the Internet Engineering Task Force (IETF) Process
- DARPA Funded Research Defined Requirements and Provided Research Implementation

Joint Government & Industry Support for Reference Implementation

- Government Focus
  - Security Enhancements
  - Improved Operations and Tools
  - Standards Compliance
- Industry Focus (Compaq, HP, IBM, Sun, SGI, Process Software, NIlabs)
  - New Functionality
  - Performance Enhancements
  - Multiprocessor Support

BIND-v9: New IETF Standards compliance

- DNSSEC
  - Required for Data Authenticity & Integrity
- [Secure] Dynamic Updates
  - Required for Mobile Users and Dynamically Configured Hosts
- IPv6
  - Required for Next Generation Internet Protocol
- EDNS0
  - To allow larger datagrams

New BIND-v9: Operational Requirements

- Large, Rapidly Growing DNS Usage
  - Huge Increase in Number of DNS Users
  - Size and Number of DNS Zones Growing Rapidly
  - Extendable to Back End Data Base
- Increasing Complexity of DNS
  - New Standards Drive More Complex DNS Questions & Answers

BIND (v9): Functional Requirements

- Provide Capability to Generate Single Answer from Multiple, Partial Answers
  - Required for IPv6 Address Derivation and DNSSEC
- Improve Distribution of DNS Processing
  - Provide Secure DNS Resolver that can Reuse Previous Answers
- Provide Incremental Transfer of DNS Zone Data

BIND (v9): Performance Enhancements

- Support for Multiprocessor Systems
  - Needed for Heavily Loaded Servers
- Support for Multiple Thread Processing
  - Needed to Process Complex Answers
- Improved Internal Data Structures
  - Reduces Format Conversion Load
- Enhanced Storage Format for DNS Files
  - Needed for Rapid Restarts

DNS Security Ingredients

- DNS Security Extensions
  - KEY and SIG resource records
  - NXT resource records
- Query-Response Security
  - TSIG and SIG(0) meta records
  - TKEY meta record
- Serving Security Data
  - CERT(ificate) resource record
- Dynamic Update Security
  - authorization of updates

Features

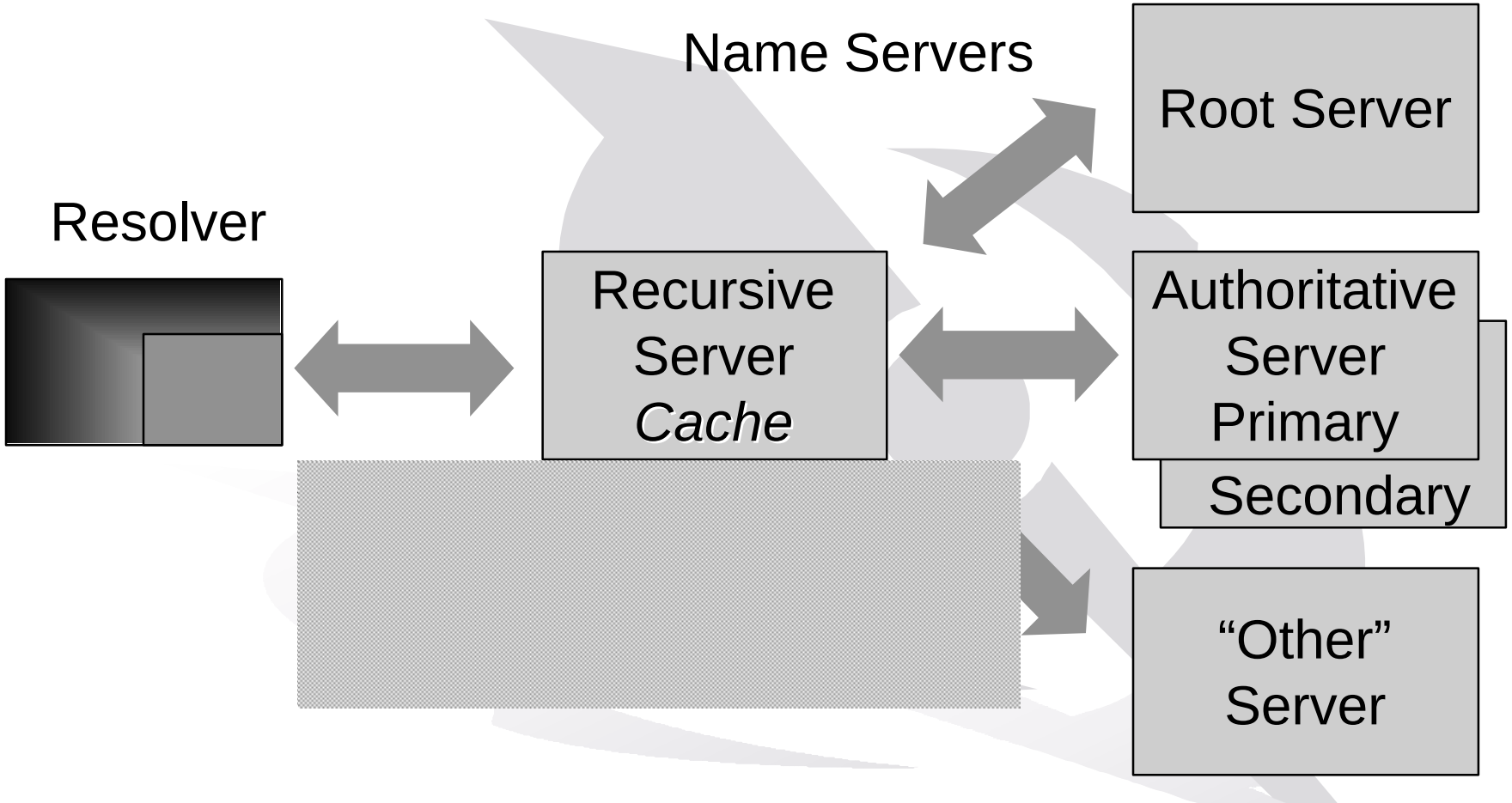
- Protection of Internet-scale DNS data transfers
  - Data is signed using scaleable public keys
  - Absent data notices (e.g. NXDOMAIN) secured
- Protection of local DNS transfers
  - Entire message secured (header and data)
- Public Key Infrastructure
  - Look up keys instead of trusting "what is heard" or manually entered
- Secured dynamic updates to zones
  - Authorized changes to zone data can be made

Deployment Plans

- Major push in Europe
  - Three ccTLD's plan to have signed zones by first quarter next year, one as soon as 31/12/2000
  - CENTR has a DNSSEC WG in action
- Root Servers
  - Looking into adoption, sooner rather than later
  - Need BIND 9 to be out & stable first
- U.S.
  - Nothing firm, just some "interest"
- Deployment experience is needed to evaluate the current protocol definition

DNS Terminology

Things to keep in mind



DNS RRs and RR sets

Things to keep in mind

- <owner> <ttl> <class> <type> <rdatalen> <rdata>
  - myname.xy. 14400 IN A 123.123.123.123
  - myname.xy. 14400 IN A 203.123.245.123
- In DNS today
  - Records with common owner, type, class are treated together, but still are singular entities
- For DNSSEC
  - The RR set is formalized
  - No longer are records singular, always treated as a set

* So, I will be talking about "sets" of data

Zones vs. Servers

Things to keep in mind

- Zone is an administrative cut of the name space
- Name server is a host dispensing information
- Relationship
  - A zone is served by name servers (1 or more)
  - A name server may serve many zones (0 or more)
  - Authoritative servers have the original zone data
  - Primary master server has the data in a source text file

* DNSSEC secures on the basis of zones

* Query/Response secures between a resolver and a server

  - Or, in the case of zone transfers, between two servers

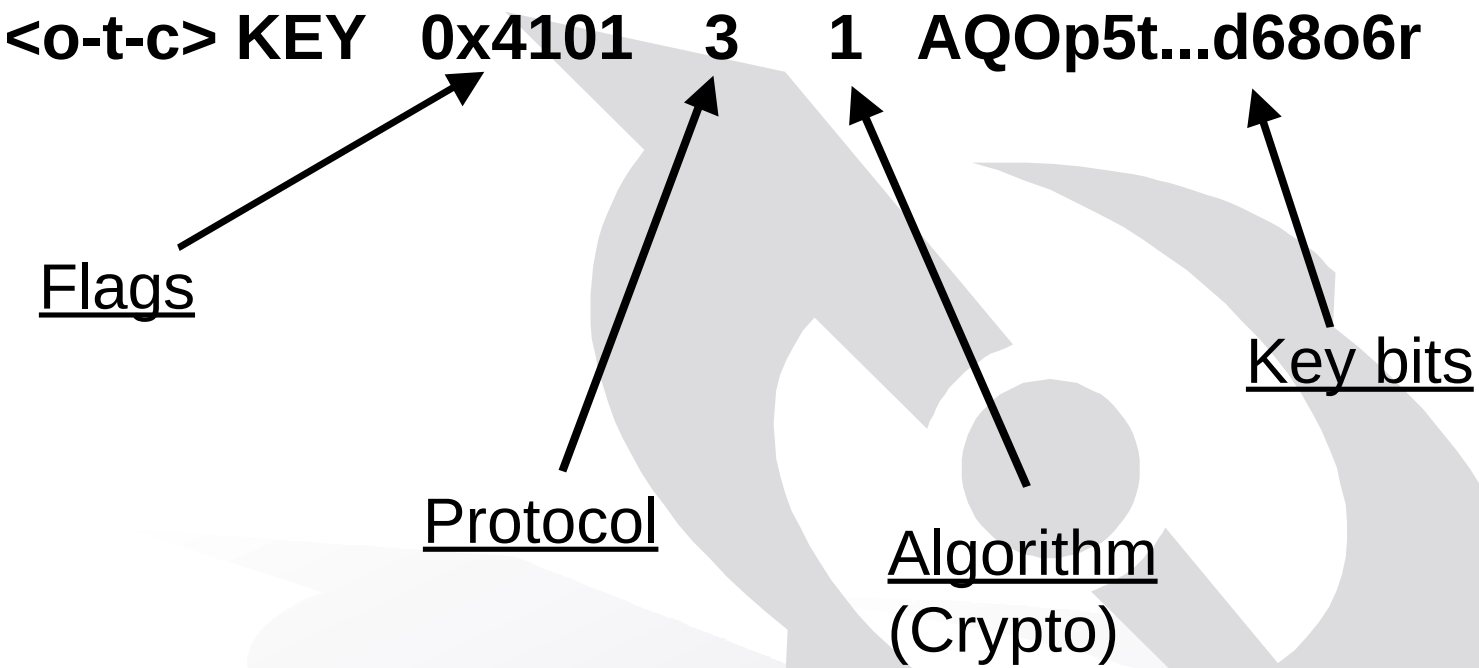
network ASSOCIATES

DNS Security Extensions

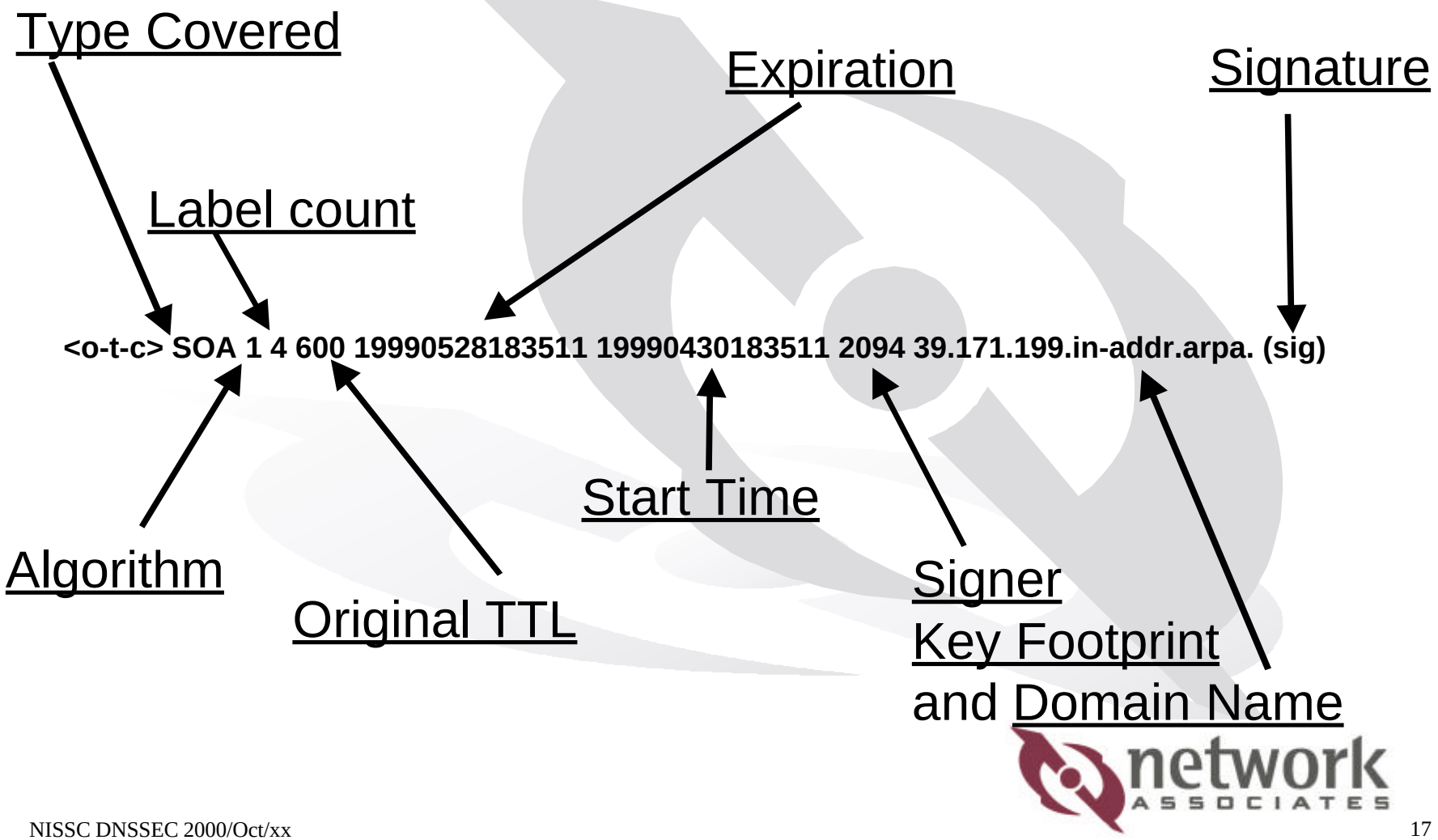
Start of "details"

- Protecting data transfers in which scalability is critical
  - I.e., inter-server queries
- Resource records introduced
  - SIG holds a digital signature (asym. keys)
  - KEY holds a public key
  - NXT indicates data present and next name

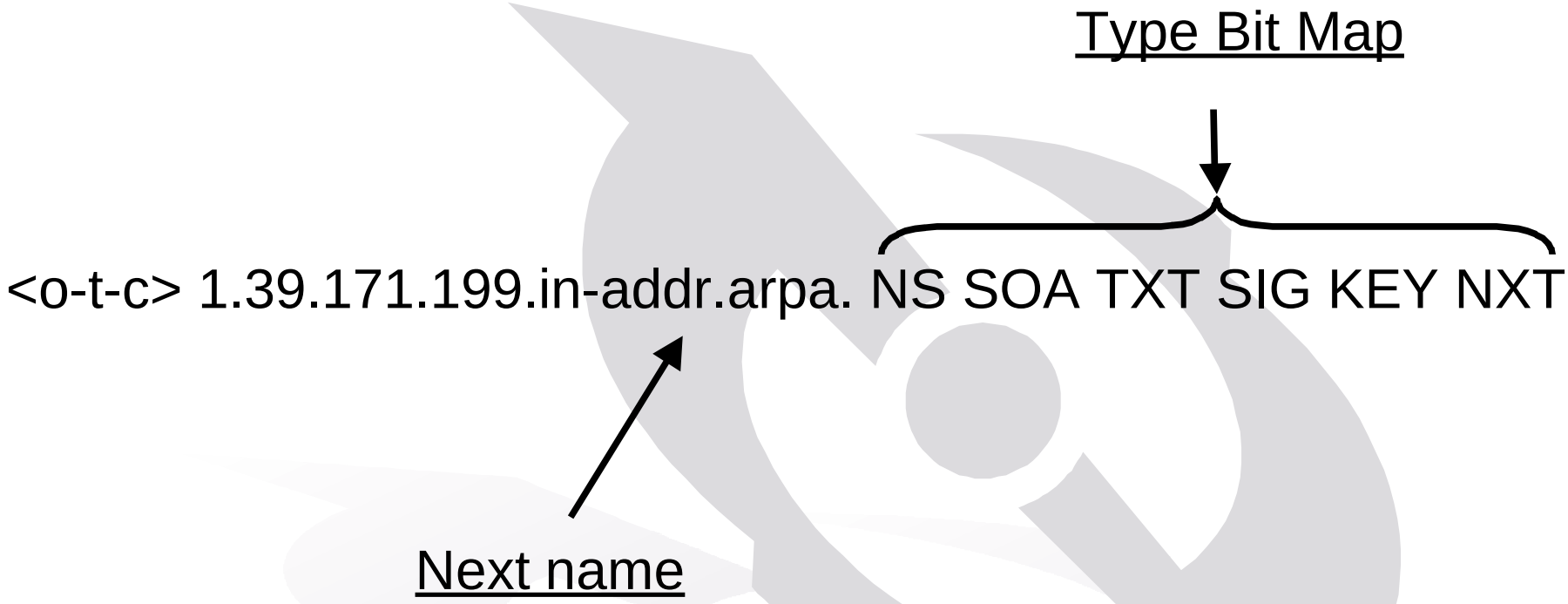
The KEY RR


<o-t-c> KEY 0x4101 3 1 AQOp5t...d68o6r
Flags
Protocol
Algorithm
(Crypto)
Key bits

The SIG RR

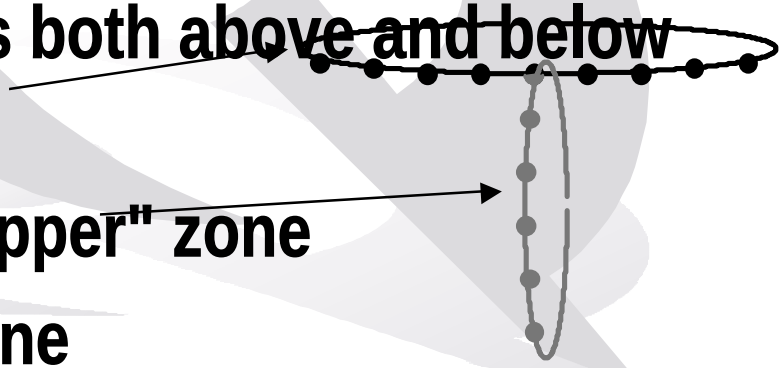

Type Covered
Expiration
Signature
Label count
<o-t-c> SOA 1 4 600 19990528183511 19990430183511 2094 39.171.199.in-addr.arpa. (sig)
Start Time
Algorithm
Original TTL
Signer
Key Footprint
and Domain Name

The NXT RR


Type Bit Map
<o-t-c> 1.39.171.199.in-addr.arpa. NS SOA TXT SIG KEY NXT
Next name

A quirk of NXT

- The NXT record indicates the data sets present at the owner's name
- It also indicates the next name in the zone
- There is one NXT for most names, but delegation names have two
  - A delegation name appears both above and below the cut point
  - One NXT belongs to the "upper" zone
  - The other to the "lower" zone
- NXT's are not generally "loved"



A signed zone, page 1

- **This example shows the KEY, SIG, and NXT RRs**

```
; Generated by dns_signer dated October 18, 1999
$ORIGIN tise.cairn.net.
@ 14400 IN    SOA   test.netsec.tislabs.com. lewis.tislabs.com. 2000020701 1D 1H 1W 4H
  14400 IN    SIG   SOA 3 3 14400 20000306184745 20000207184745 48320 tise.cairn.net. (
                    AIrF9Hb/BzoZ3xir1K81xLzprIEVBFZLEE6Sqy8HlaU5r3ux
                    VfBbcTA= )
  14400 IN    KEY   0x4100 3 3 (
                    ALb/qZQ/oVHyotuSbBWI1N+OYwRLv5RMc7XXb0wYE/tY02qF
                    Uf+9czS0B7pU2jYppF7RwL8b/OcWG3iAzaztzq6S0ZoQIh8J
                    M5LummzJiNl3aqxDxUZH6pwmPNuiMbGl++2tUks+MAallpUz
                    4tEJPeBF+Zj8boYwWhQDaV6nwDY6kIrqRqhvAmOZHqtqzFT6
                    SdA07usEZEzZkXXS6PIg6JcN7mNhUa0qkDSNTIkrHWNCh++G
                    56dtKNxk4qn3ESreg/S2BRGWQ2/7X0PjMyBkDefvdIsw )
  14400 IN    SIG   KEY 3 3 14400 20000225145656 20000128145656 48320 tise.cairn.net. (
                    AKM6fdJmcV3Wec7sYKR5ktX2C3kWTLTcITD4iBP2rJVSF1Kx
                    nsi3bRI= )
```

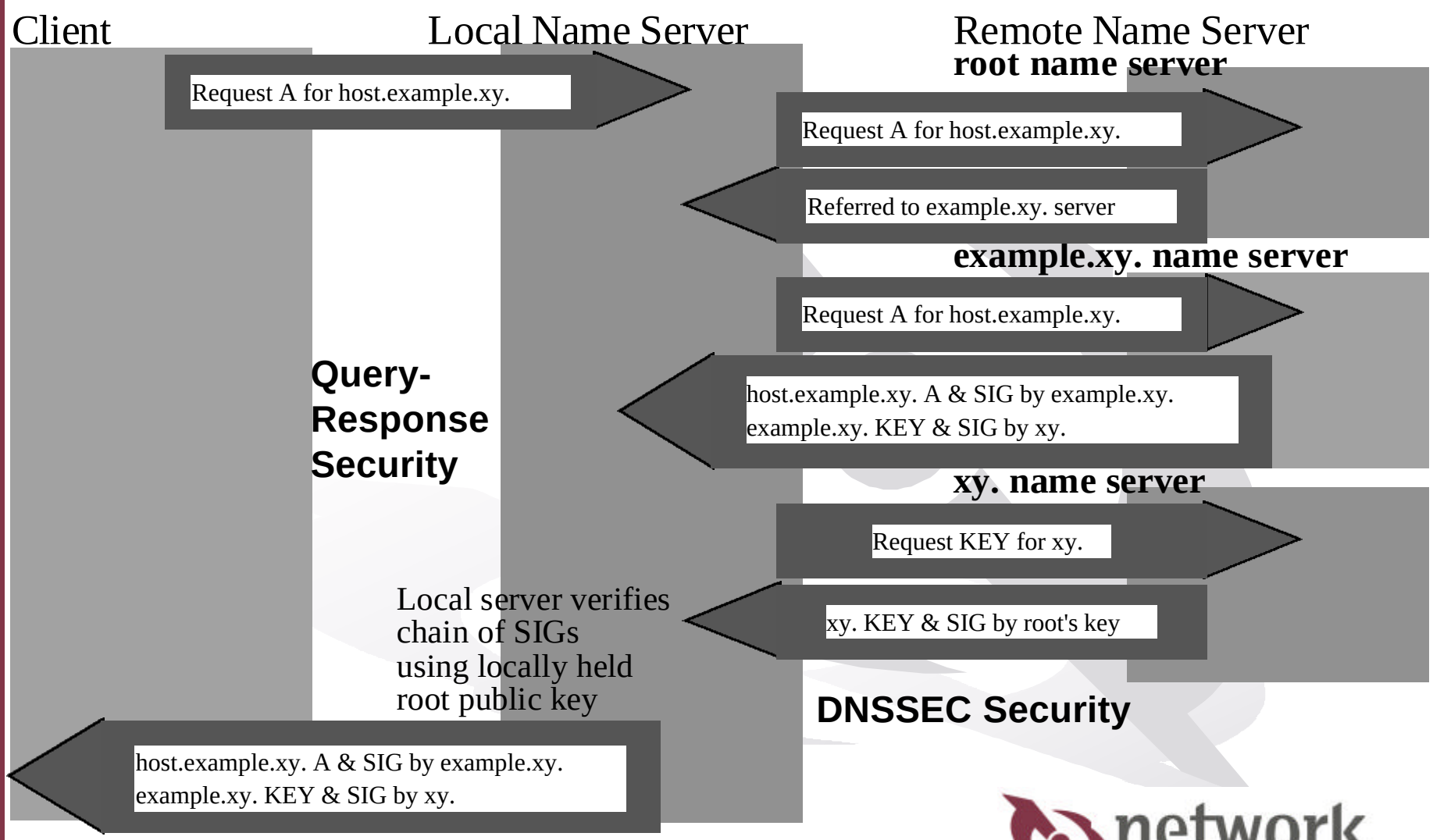
...continues on next slide...

A signed zone, page 2

```
@       14400 IN NS     buddy.netsec.tislabs.com.
        14400 IN NS     active.netsec.tislabs.com.
        14400 IN NS     test.netsec.tislabs.com.
        14400 IN SIG    NS 3 3 14400 20000225145656 20000128145656 48320 tise.cairn.net. (
                        AKqbf3kRV1P63jDVS96dq9dMB/OXjLw0FDtdUuyVIq2Q3Z23Ep5835k= )
        14400 IN NXT    active.tise.cairn.net. NS SOA SIG KEY NXT
        14400 IN SIG    NXT 3 3 14400 20000225145656 20000128145656 48320 tise.cairn.net. (
                        AHZaL7BjH0l2VULlQJb6gXIsXjRhICsWvMapVfP2qBrGMGYl3c7yIk8= )
active  14400 IN CNAME  active.netsec.tislabs.com.
        14400 IN SIG    CNAME 3 4 14400 20000225145656 20000128145656 48320 tise.cairn.net. (
                        ACqtgIY8TkwTw83rQmt3f0P0x+TmpcCtCz1+EsFmYybcSY0lhP2Nht4= )
active  14400 IN NXT    amp.tise.cairn.net. CNAME SIG NXT
        14400 IN SIG    NXT 3 4 14400 20000225145656 20000128145656 48320 tise.cairn.net. (
                        AC75idNrAm5O1YUS1ZBD9ecDgEDdFWlWN+etN74AqVoDlhtYW8dmWeo= )
amp     14400 IN NS     test.netsec.tislabs.com.
        14400 IN NS     active.netsec.tislabs.com.
        14400 IN NS     buddy.netsec.tislabs.com.
amp     14400 IN NXT    buddy.tise.cairn.net. NS SIG KEY NXT
        14400 IN SIG    NXT 3 4 14400 20000225145656 20000128145656 48320 tise.cairn.net. (
                        ADg3LFw5GvcFHgC7UaCZrK/rn5IVOg8ddTgkWz9PK9Z1KvToQbNZ3NQ= )
```

....and there's still more to the zone, not shown

DNSSEC Queries



Going secure

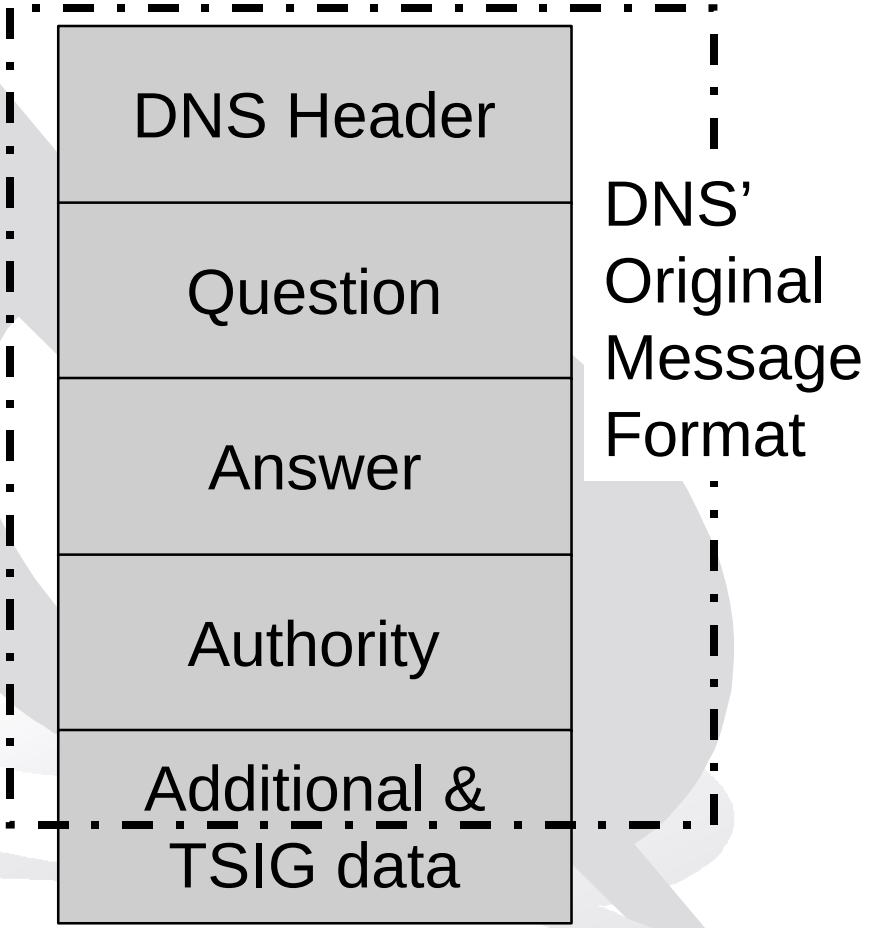
- Preparation (not necessarily in order)
  - A "secured" zone begins with an "unsecured" zone
  - Zone key pair generated and validated by parent
  - SIG records generated for each set in zone
  - NXT and SIG(NXT) are generated and added
- Running
  - Response to query includes the desired set(s), the SIG (set), and possibly KEY and SIG(KEY)'s that will help the resolver evaluate the answer
  - There are many variations on this, this is the general theme

Query/Response Security

- Processing power is a greater issue than scalability
  - This includes lightweight resolver queries to a "preferred" server
  - Zone transfers (AXFR)
  - A basis for securing dynamic update
- (Meta-) Resource records introduced
  - TSIG/SIG(0)
  - TKEY

TSIG

- A "keyed hash" covering entire DNS message
  - Uses a shared secret, shared between resolver and server
- Messages covered
  - query - response
  - zone transfer
  - dynamic updates



TSIG Notes

- Storage of shared secret is an issue
  - No problem for named.conf, it can be protected
  - Problem for resolv.conf
  - TKEY is a proposed method for creating TSIGs
- Early use of TSIG
  - Zone transfers
  - "Special" clients (e.g., DHCP updaters)
- Widespread use later
  - Once overhead of sharing secrets is reduced

TSIG in configuration files

- **Primary server**

options {...;};

```
key "test" {
   algorithm hmac-md5;
   secret "ThePlaceToBe";
};
server 10.33.40.35 {
   keys {test;};
};
```

- **Secondary server**

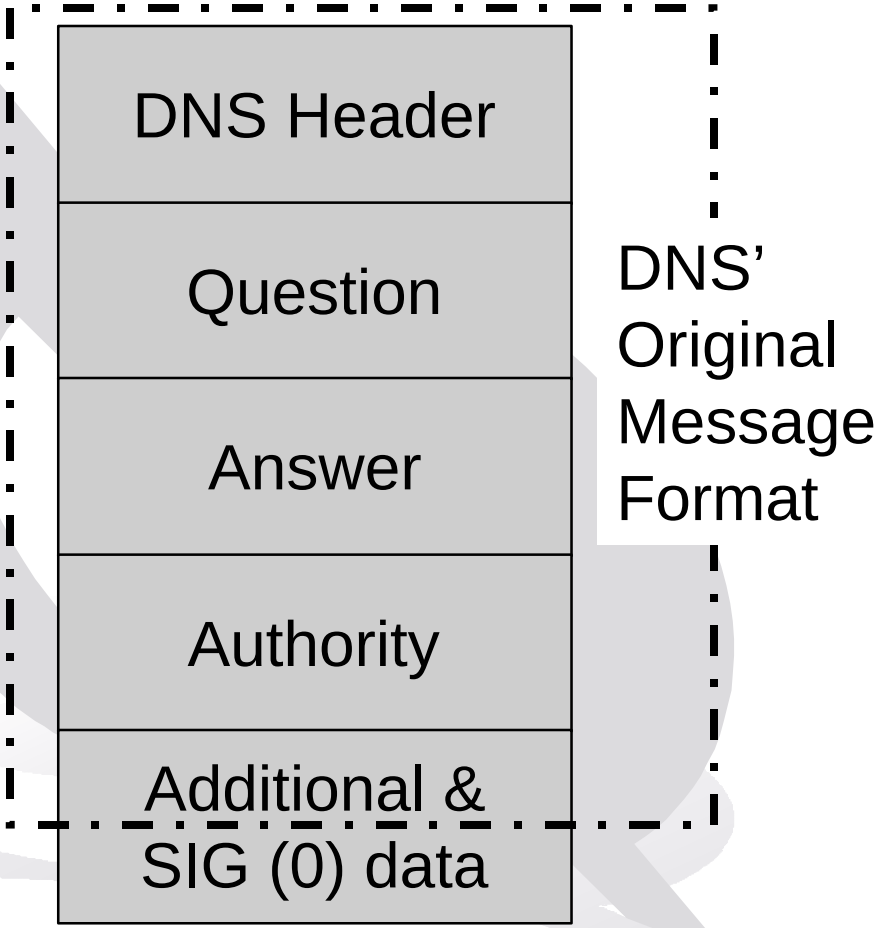
options {...;};

```
key "test" {
   algorithm hmac-md5;
   secret "ThePlaceToBe";
};
server 10.33.40.46 {
      keys {test;};
};
```

network ASSOCIATES

SIG(0)

- Functionally equivalent to TSIG
  - Uses asymmetric keys instead of shared secret
- Messages covered
  - query - response
  - zone transfer
  - dynamic updates

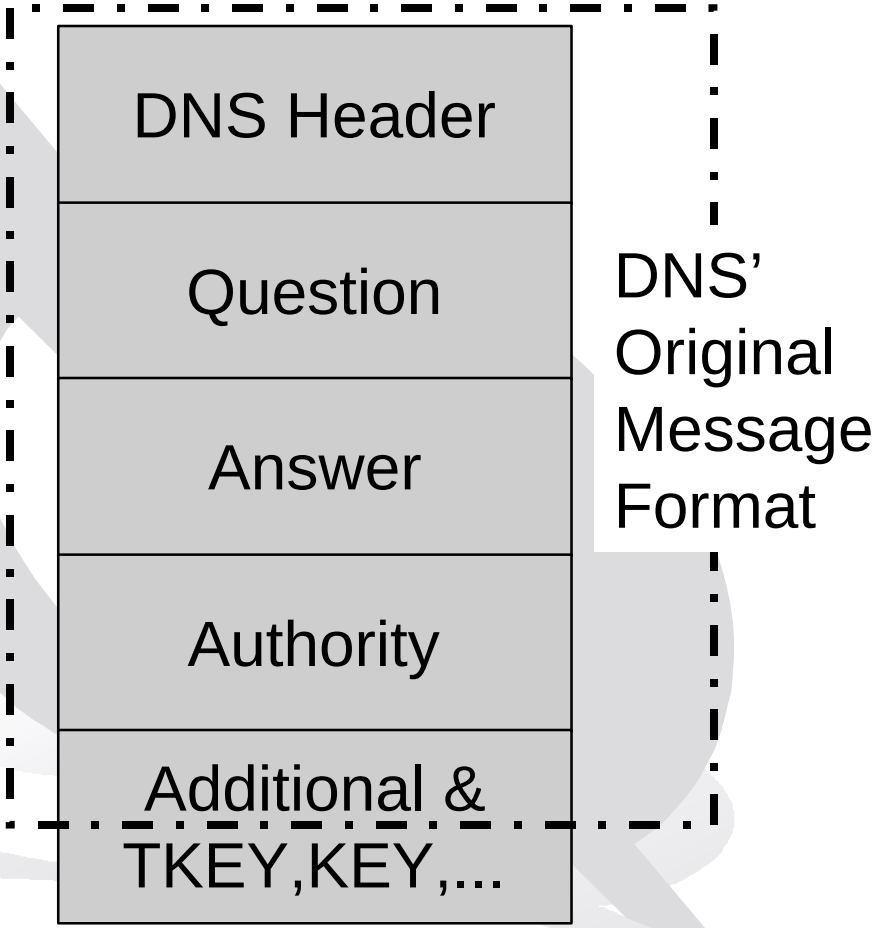


SIG (0) Notes

- Defined in RFC 2535 w/KEY, SIG, and NXT
  - A current Internet Draft fixes the specification
- SIG(0) requires a public key to be in a zone
- Suffers performance hit of public key cryptography
  - Useful where performance hit isn't as bad as overhead managing shared secrets
- Requires client to have a private key available to the resolver

TKEY

- **Sent in a request to create a TSIG shared secret**
- **Request is accompanied by a KEY from which to generate the shared secret**
- **This is an example of the optimization on the "Cryptography" slide (#11)**



TKEY Notes

- TKEY is sent by resolver to set up a TSIG with server
  - Diffie-Hellman mode
  - GSSAPI - in Windows 2000
  - Server or Client assigned (no implementations)
- A TSIG is set up and used in subsequent queries and responses
- Unsigned DH TKEY requests can pose a denial of service threat
  - Allowing "anonymous" TKEY is dangerous because of the CPU load induced

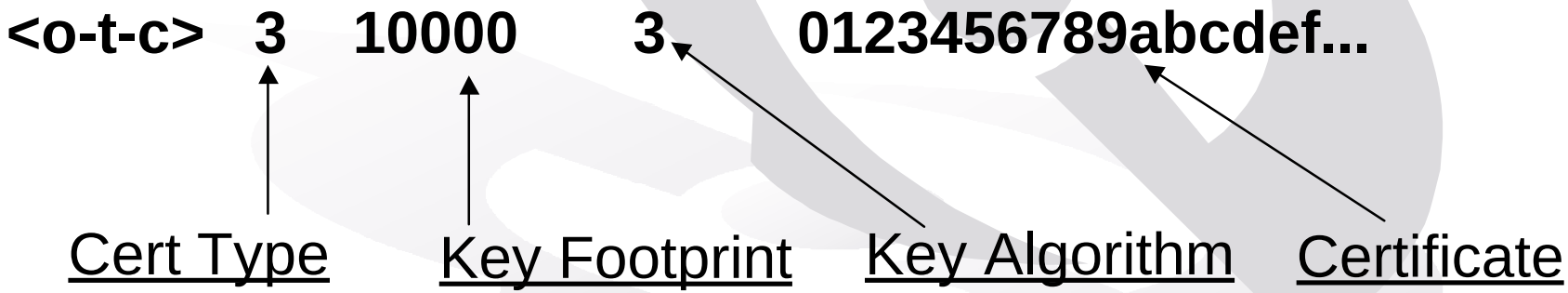
Security Data Server

- DNS can provide a public, scaleable, redundant mechanism to pass public security data
  - Certificates & Public Keys
- DNSSEC validation of data has limits
  - DNSSEC provides that "what you see is what I sent"
  - DNSSEC does not provide assurance that the contents were entered correctly
- Resource record introduced
  - CERT(ificate)

network ASSOCIATES

The CERT RR

- Certificates are a means to bind a public key to an identity with conditions
- DNS CERT RR's can store different kinds of certificates (X.509, SPKI, PGP)
- Software to make the RR's is still lacking



Securing Dynamic Update

- Still in definition (in IETF Last Call)
- BINDv9 implements Secure Update
  - TSIG or SIG(0) covered messages identify the requestor
  - The name server holds an authorization matrix indicating whether the requestor is allowed to make the requested change
  - Granularity of the policy is being defined, some defaults are being identified, rest is up to admin

Impact

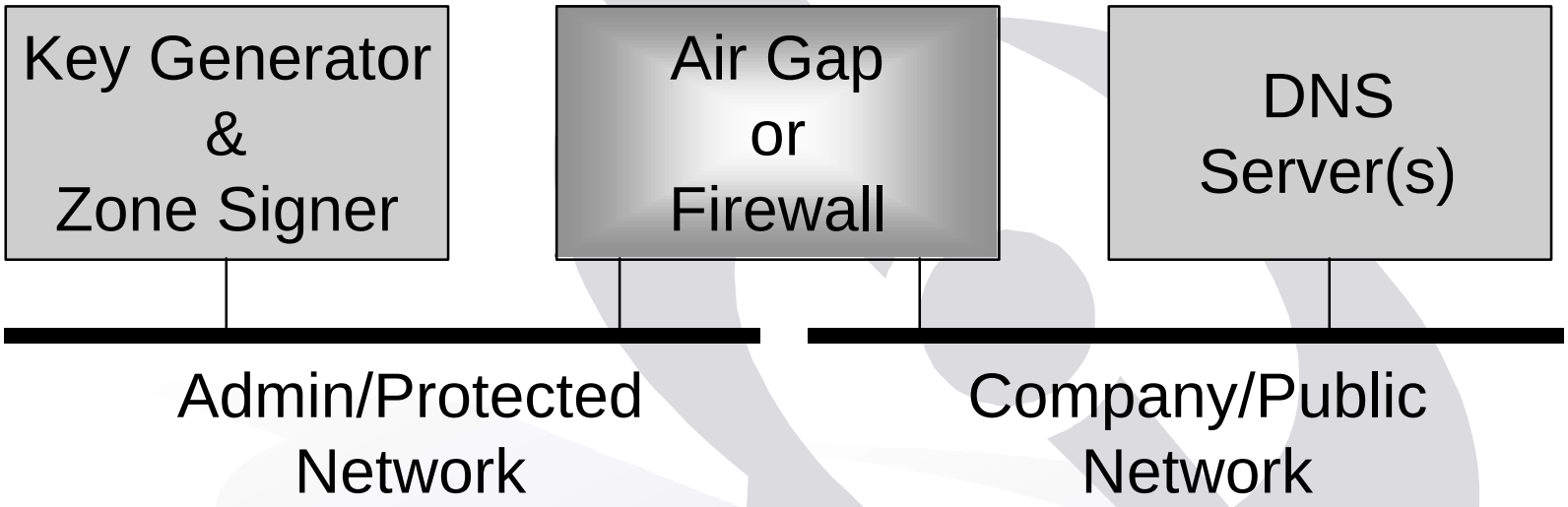
- DNSSEC will increase attention paid to DNS
  - Data (SIG) "expires" from the authoritative server
    - No more "load & forget"
  - Delegations have a recurring relationship
  - Administrators have to manage keys
    - NOC procedures needed for this
  - Need more resources (CPU) to run

Validating Delegations

- Validation of a zone's keys by its parent is important
  - Provides "proof" of zone delegation
  - Relationship between delegations be interactive
- Work is progressing on automating this
- Will this help keep registry info current?

Off-line Signing

T he DNSSEC specification refers to "off-line signing'



Reason: Protect the Private Key(s)
Secure Dynamic Update complicates this
Issue: Will this be done?